



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

| APPLICATION NO.                                                           | FILING DATE | FIRST NAMED INVENTOR      | ATTORNEY DOCKET NO.         | CONFIRMATION NO.       |
|---------------------------------------------------------------------------|-------------|---------------------------|-----------------------------|------------------------|
| 10/627,281                                                                | 07/25/2003  | Anne Kirsten Eisentraeger | MS1-1275US                  | 4249                   |
| 22801                                                                     | 7590        | 01/11/2008                |                             |                        |
| LEE & HAYES PLLC<br>421 W RIVERSIDE AVENUE SUITE 500<br>SPOKANE, WA 99201 |             |                           | EXAMINER<br>PEESO, THOMAS R |                        |
|                                                                           |             |                           | ART UNIT<br>2132            | PAPER NUMBER           |
|                                                                           |             |                           | MAIL DATE<br>01/11/2008     | DELIVERY MODE<br>PAPER |

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

## Office Action Summary

**Application No.**

10/627,281

**Applicant(s)**

EISENTRAEGER ET AL.

**Examiner**

Thomas R. Peeso

**Art Unit**

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

### Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on amendment filed on 09Oct2007.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-44 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-3, 5, 7-10, 18, 19, 21-23, 31-33 and 35-37 is/are rejected.
- 7) ☒ Claim(s) 4, 6, 11-17, 20, 24-30, 34 and 38-44 is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 26Jul2003 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
- Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- |                                                                                      |                                                                   |
|--------------------------------------------------------------------------------------|-------------------------------------------------------------------|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892)                     | 4) <input type="checkbox"/> Interview Summary (PTO-413)           |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____                                      |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08)          | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____                                                          | 6) <input type="checkbox"/> Other: _____                          |

### DETAILED ACTION

#### Claim Rejections - 35 USC § 102

Claims 1,2, 3, 5, 7, 8, 9,10, 18, 19, 21, 22, 23, 31, 32, 33, 35, 36, 37 are rejected under 35 U.S.C. 102(e) as being anticipated by Lenstra, USpatent6446205.

In reference to claim 1:

Lenstra discloses a method for use in curve-based cryptographic logic, the method comprising:

- Determining at least one curve for use in cryptographically processing selected information, where the participant chooses a curve for use in the cryptosystem (Column 3, lines 14-20)

•  
Determining pairings for use in cryptographically processing said selected information by selectively using at least one parabola associated with said at least one curve, where the parabola is an elliptic curve, and wherein the pairings are sets of elliptic curve equations. (Column 3, lines 14-20) & (Column 3, lines 30-Column 4, line 43)

In reference to claim 2:

- Lenstra (Column 3, lines 15-67) discloses the method as recited in claim 1, wherein said at least one curve includes an elliptic curve. (Column 3, lines 50-53)

In reference to claim 3:

Lenstra discloses the method as recited in claim 1, wherein said pairings include Weil pairings. (Column 4, lines 35-45)

In reference to claim 5: Lenstra discloses the method as recited in claim 1, wherein said pairings include Tate pairings. (Column 4, lines 35-45)

In reference to claim 7:

Lenstra discloses the method as recited in claim 1, further comprising:

Cryptographically processing said selected information based on said pairings. (Column

6, lines 60 - Column 7, lines 20) where the curves are selected for the ECC

system  
(Column 3, lines 15-55) & (Figure 4)

In reference to claim 8:

Lenstra (Figure 4) & (Column 6, lines 60 - Column 7, lines 20) discloses the method as recited in claim 7, wherein cryptographically processing said selected information based on said pairings includes decrypting said selected information and outputting corresponding decrypted information.

In reference to claim 9:

Lenstra (Figure 4) & (Column 6, lines 60 - Column 7, lines 20) discloses the method as recited in claim 7, wherein cryptographically processing said selected information based on said pairings includes encrypting said selected information and outputting corresponding encrypted information.

In reference to claim 10:

Lenstra (Figure 4) & (Column 6, lines 60 - Column 7, lines 20) discloses the method as recited in claim 7, wherein cryptographically processing is configured to support at least one process selected from a group of processes comprising a key-based process, an identity based encryption process, a product identification (ID)-based process, and a short signature -based process, where the process is a key based process and an identity based encrypted process, and a short signature based process. (Column 6, lines 1-35)

Claim 18 is rejected for the same reasons as claim 1.

Claim 19 is rejected for the same reasons as claim 2.

Claim 21 is rejected for the same reasons as claim 8.

Claim 22 is rejected for the same reasons as claim 9.

Claim 23 is rejected for the same reasons as claim 10.

Claim 31 is rejected for the same reasons as claim 1.

Claim 32 is rejected for the same reasons as claim 2.

Claim 33 is rejected for the same reasons as claim 8.  
Claim 35 is rejected for the same reasons as claim 8.  
Claim 36 is rejected for the same reasons as claim 9.  
Claim 37 is rejected for the same reasons as claim 10.

***Allowable Subject Matter***

Claims 4, 6, 11-15, 17, 20, 24-30, 34, 38-44 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

**THIS ACTION IS MADE FINAL.**

Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

**Conclusion**

Any inquiry concerning this communication from the examiner should be directed to Thomas Peeso whose telephone number is (571)272-3809. The examiner can normally be reached on M-F from 7:00 AM – 3:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (571)272-3799.

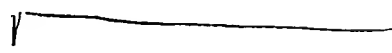
The Examiner may also be reached through email through [tpees@uspto.gov](mailto:tpees@uspto.gov)

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (571)272-2100.

General Information/Receptionist Telephone: 571-272-2100 Fax: 571-273-8300

Customer Service Representative Telephone: 571-272-2100 Fax: 571-273-8300

26 Dec 2007

  
Thomas Peeso  
Primary Examiner